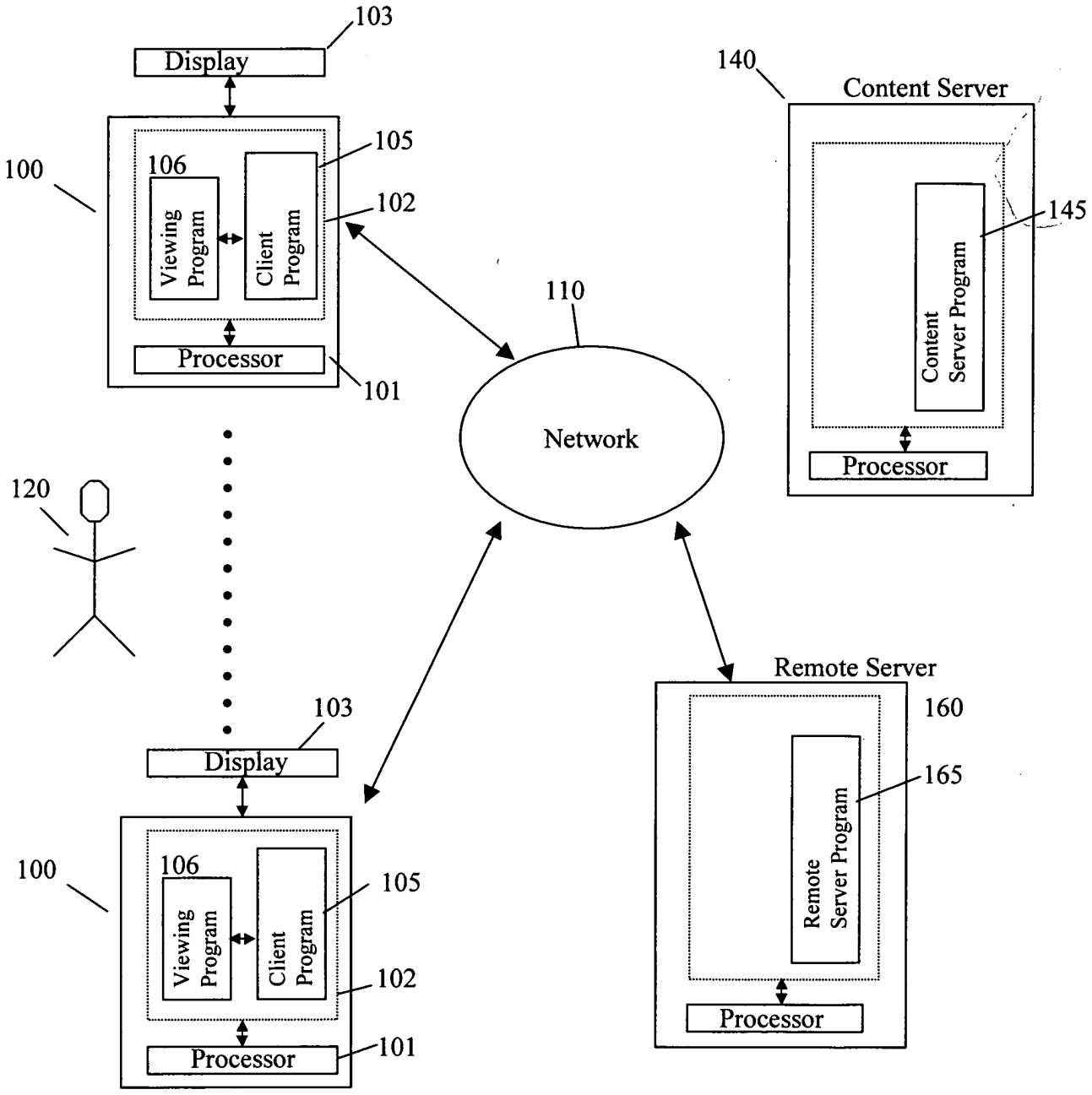
103
Display
140
Content Server
105
100
106
102
Viewing Program
Client Program
145
Content Server Program
110
Processor
101
Network
Processor
120
Remote Server
160
103
Display
165
Remote Server Program
100
106
105
Viewing Program
Client Program
102
Processor
101

Fig. 1

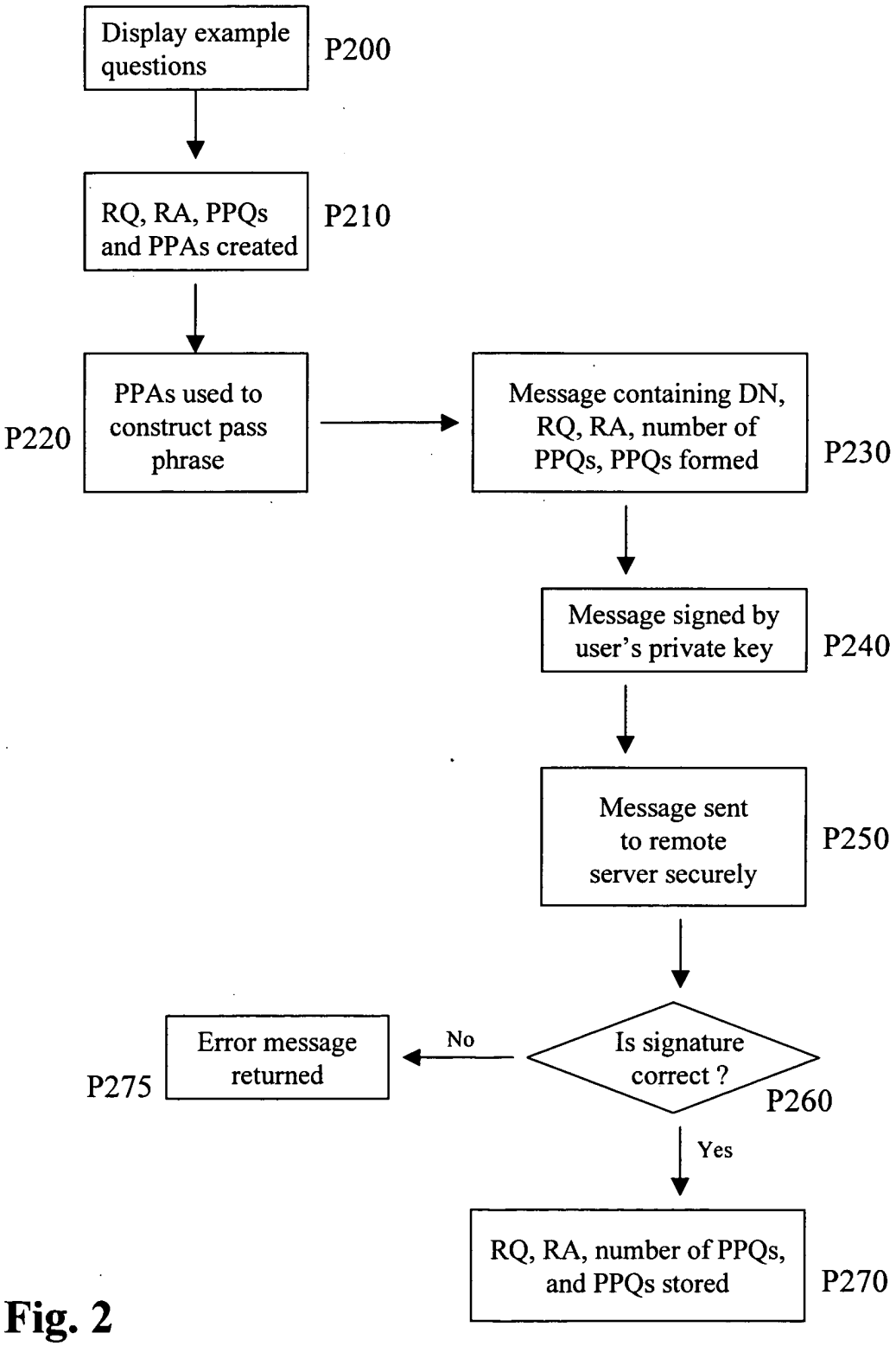
Display example questions
P200
RQ, RA, PPQs and PPAs created
P210
P220
PPAs used to construct pass phrase
Message containing DN, RQ, RA, number of PPQs, PPQs formed
P230
Message signed by user's private key
P240
Message sent to remote server securely
P250
Is signature correct ?
P260
No
Error message returned
P275
Yes
RQ, RA, number of PPQs, and PPQs stored
P270

Fig. 2

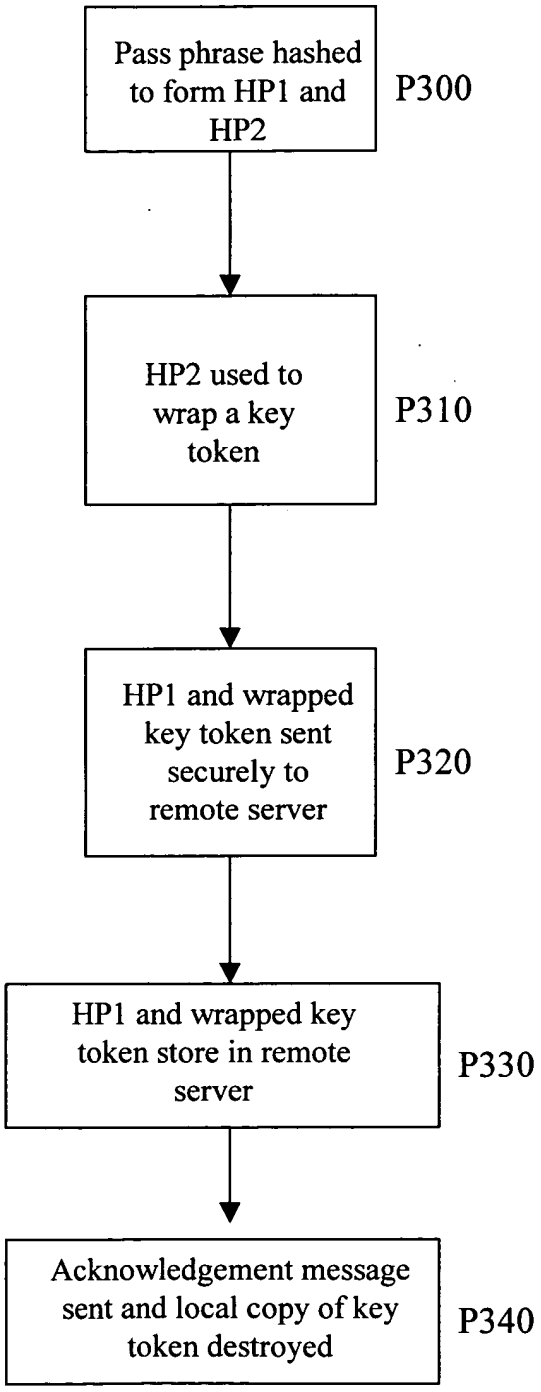
Pass phrase hashed to form HP1 and HP2
P300
HP2 used to wrap a key token
P310
HP1 and wrapped key token sent securely to remote server
P320
HP1 and wrapped key token store in remote server
P330
Acknowledgement message sent and local copy of key token destroyed
P340

Fig. 3

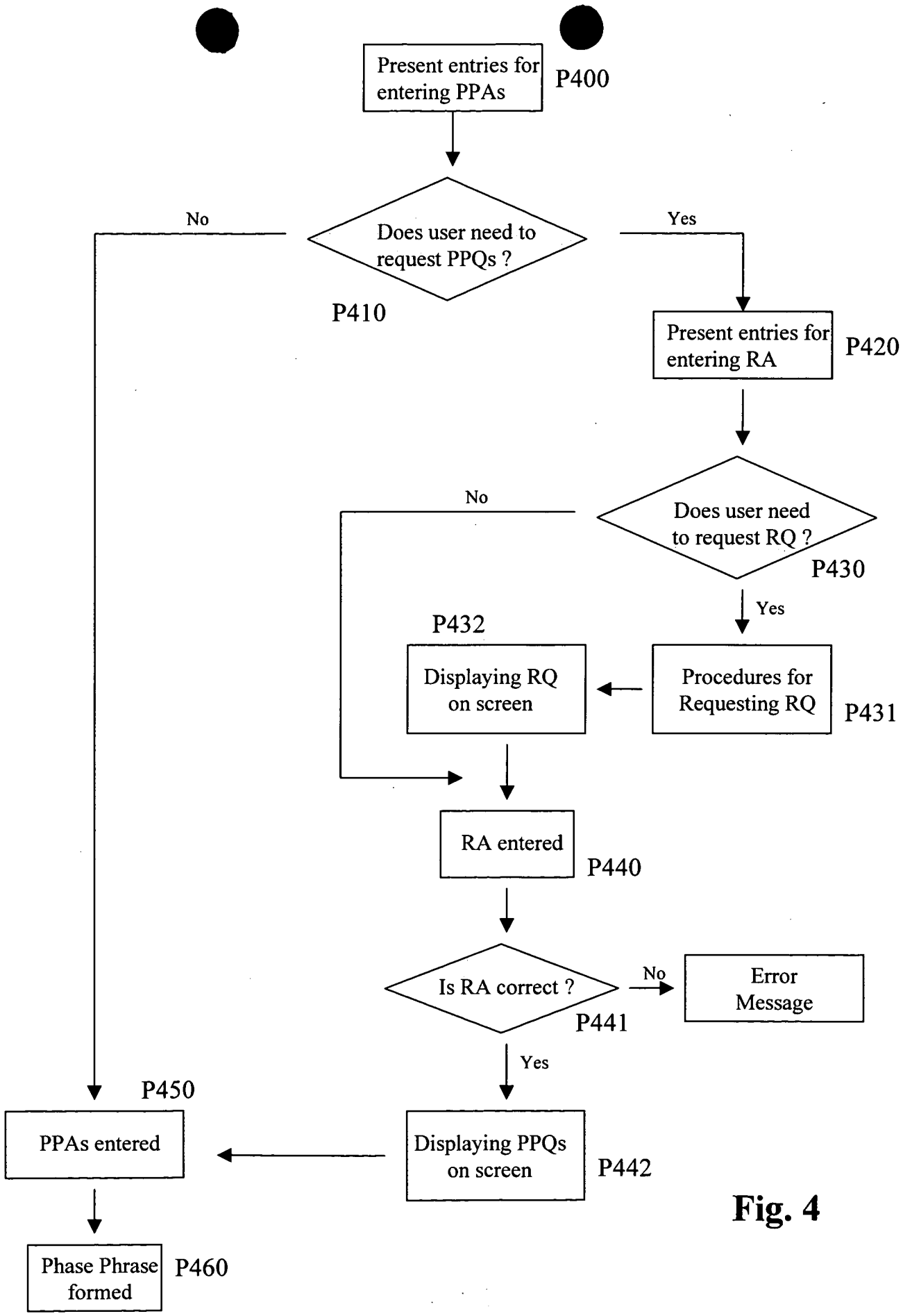
Present entries for entering PPAs
P400
Does user need to request PPQs ?
P410
No
Yes
Present entries for entering RA
P420
Does user need to request RQ ?
P430
No
Yes
P432
Displaying RQ on screen
Procedures for Requesting RQ
P431
RA entered
P440
Is RA correct ?
P441
No
Error Message
Yes
P450
PPAs entered
Displaying PPQs on screen
P442
Phase Phrase formed
P460

Fig. 4

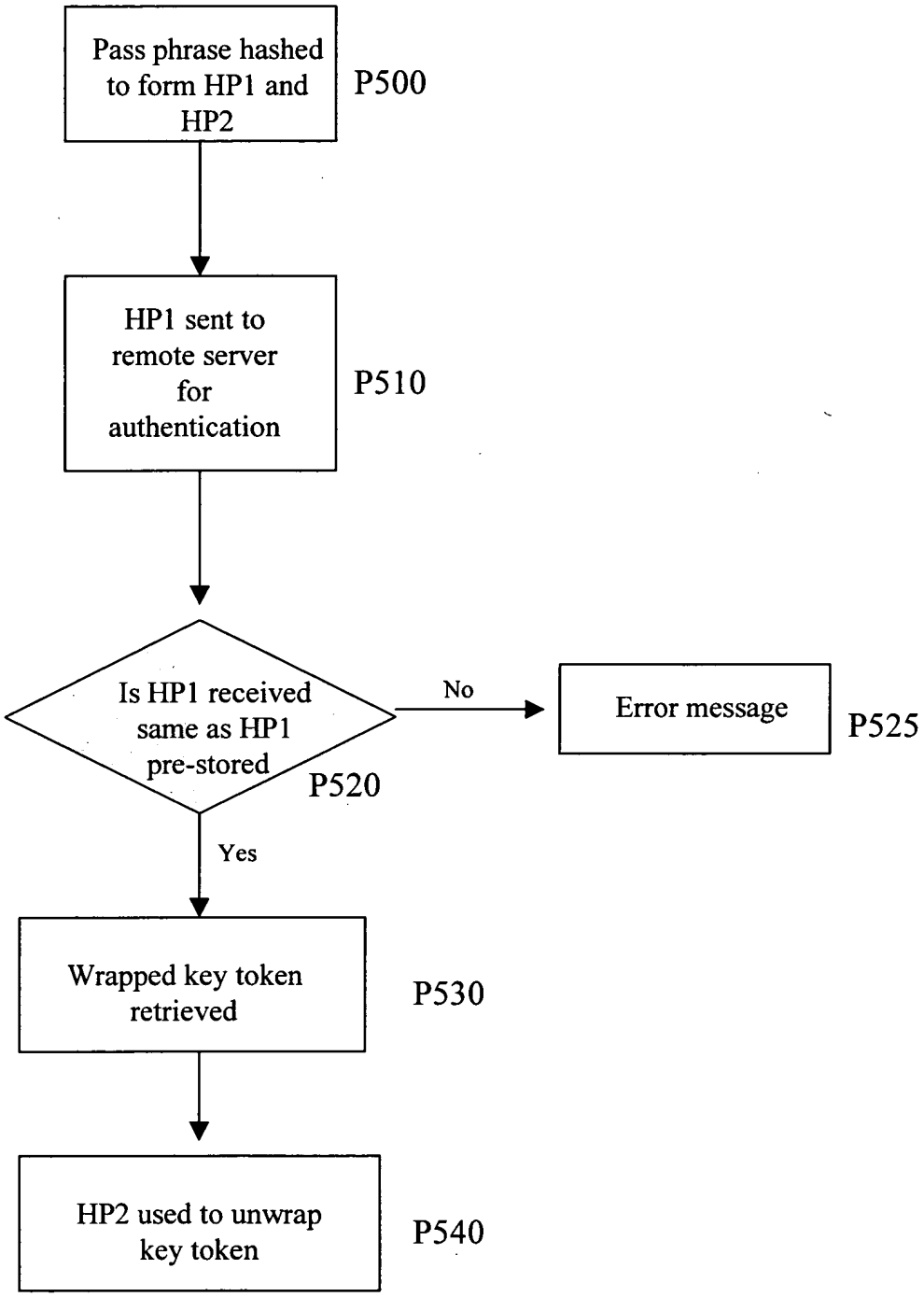
Pass phrase hashed to form HP1 and HP2
P500
HP1 sent to remote server for authentication
P510
Is HP1 received same as HP1 pre-stored
P520
No
Error message
P525
Yes
Wrapped key token retrieved
P530
HP2 used to unwrap key token
P540

Fig. 5

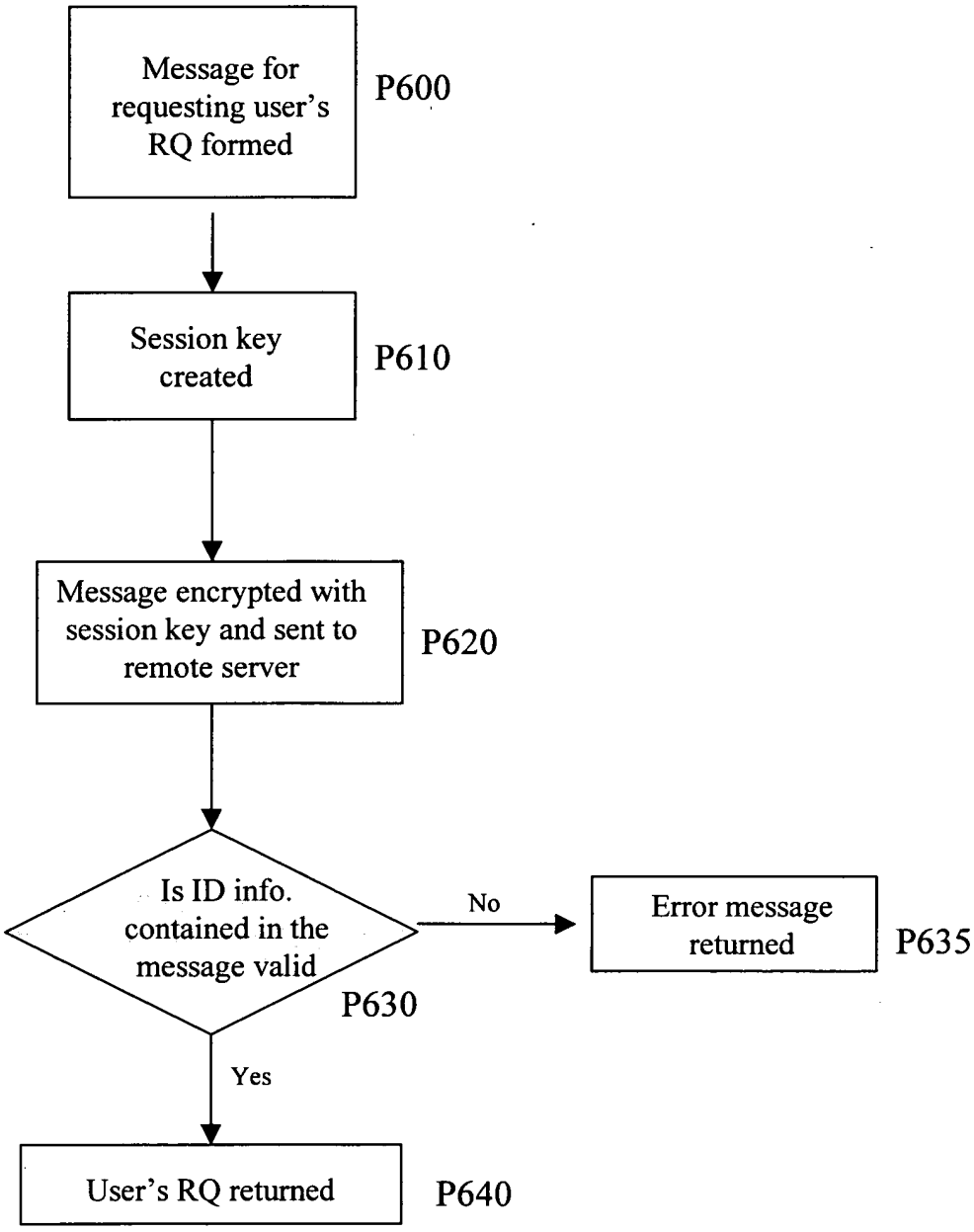
Message for requesting user's RQ formed
P600
Session key created
P610
Message encrypted with session key and sent to remote server
P620
Is ID info. contained in the message valid
P630
No
Error message returned
P635
Yes
User's RQ returned
P640

Fig. 6

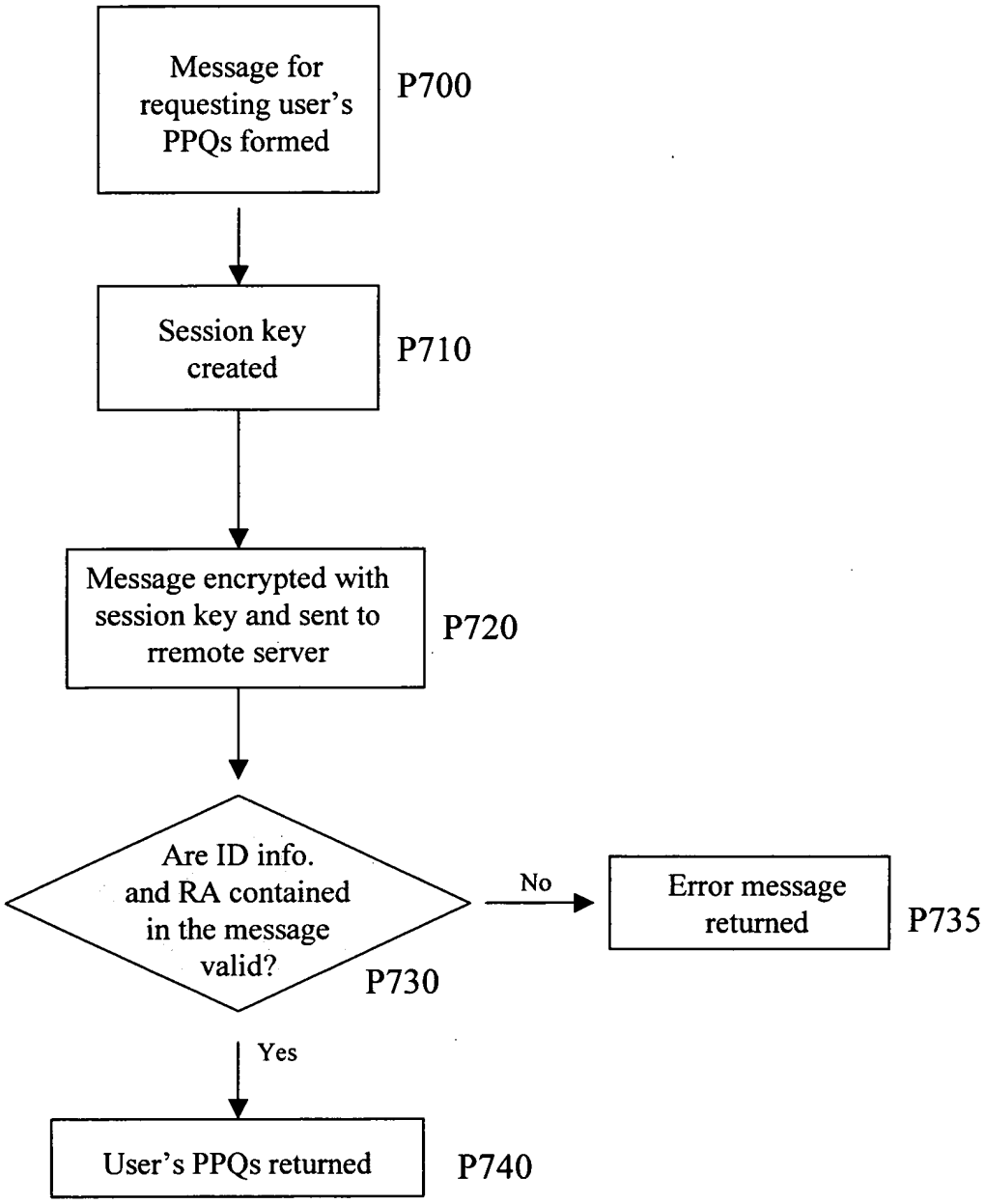
Message for requesting user's PPQs formed
P700
Session key created
P710
Message encrypted with session key and sent to rremote server
P720
Are ID info. and RA contained in the message valid?
P730
No
Error message returned
P735
Yes
User's PPQs returned
P740

Fig. 7